WHAT IS CLAIMED IS:

1. Method for securing updating data from a plurality of apparatuses, each apparatus receiving the updates from a managing center, these updates including data called patch accompanied by a control block encrypted by a private asymmetrical key taken from a list of keys included in the managing center, characterized by following steps:

- selection by means of the apparatus of a current key from a list of public keys,
- reception and storage in the memory of the updating patch,
- reception of the encrypted control block,
- decryption of said block by the current public key,
- verification that the decrypted control block corresponds to said patch,
- installation of the patch received,
- deactivation of the current key and selection of the next key in the list.

2. Method according to Claim 1 wherein the control block includes a signature on the patch data, this signature being the result of a hash function.

3. Method according to Claims 1 and 2 wherein the verification of the block includes the step of establishing the signature on the received patch and the comparison with the decrypted signature in the control block.

4. Method according to Claim 1 wherein the control block includes a symmetrical session key determined by the managing center, this key being used to encrypt the patch data.

5. Method according to Claim 1 wherein, for each update, a new public key taken from the list is used by the apparatus.

6. Method according to Claim 1, wherein the public key is deleted from the list after being used, said key being useless for the next updates.

7. Method according to Claim 1, wherein the public keys of the list are used sequentially in a predetermined order during each update.

8. Method according to Claim 1 wherein the list of public keys is stored in a non-volatile memory, a key used for an update is definitively deleted from the memory that authorizes the access to the next key for the subsequent update.

9. Method according to Claim 1 wherein, for the updating of the software of an apparatus of a certain version to a new version, with a difference between the new version and the previous one greater than one, at least one message encrypted with a private key is added allowing the changing of the current key to the next key in the list, the successful decryption of said message inducing the deactivation of the current key and the selection of the next key.

10. Method according to Claim 9, wherein the number of messages corresponds to the number of updates separating the initial version of the apparatus and the final version of the update.

11. Method according to Claim 1, wherein an updating installation is followed by an increment on a counter or by moving a pointer indicating the position of the key to be selected from the list during the subsequent update, while the list of keys remains unchanged.

12. Method according to Claim 1, wherein the control block is successively encrypted by the keys of the previous updates, each key from the list being used one after the other to decrypt the signature.

13. Method according to Claim 1, wherein the apparatuses consist of Pay-TV decoders, an update of a decoder being carried out by downloading, from a managing center, of a patch accompanied by a control block, said block is stored in a Random Access Memory, and is decrypted with a current public key contained in a first non-volatile memory of the decoder, then verified and in the case of correspondence, a command leads the installation of the patch in a second non-volatile memory and the deactivation of the current key.

14. Method according to Claim 13, wherein a new list of public keys is transmitted to the decoder, said list replaces the list contained in the first memory containing keys deactivated by previous successful updates.